

WO 2006/051791

1

PCT/JP2005/020470

明 細 書

データ再生方法及びデータ処理装置

技術分野

- [0001] 本発明は、映画などの著作物であるコンテンツをデジタル化したデータを、例えばデジタル光ディスク等の大容量メディアに格納し、特定の端末においてのみデータを完全に獲得できる方法に関連し、特に、大容量メディアに記録された、著作権を保護するために暗号化及び変形されたコンテンツデータを再生する技術に関する。

背景技術

- [0002] 近年、蓄積メディアが大容量化するに伴い、映画などの著作物であるコンテンツをデジタル化して、例えばデジタル光ディスク等のメディアに格納して配布するシステムが普及している。こうしたシステムにおいては、コンテンツの著作権が保護され、著作権者との合意による制限の下でのみコンテンツの再生や複製などが実行されることが必要となる。著作物を著作権者の許可のない不正コピー等から保護するための一般的なシステムは、デジタルコンテンツを、著作権者の管理する、あるコンテンツ鍵により暗号化し、ディスクに記録し、該当するコンテンツ鍵を持つ端末だけがこれを復号できるといった仕組みを備えている。そして、そのコンテンツ鍵を入手するためには著作権者との間で著作権保護に対する規定が義務付けられるというものである。
- [0003] そのようなシステムの一例として、特許文献1にて、コンテンツデータを暗号化、及び復号化するためのコンテンツ鍵をシード鍵と時変数データとの関数に基づいて生成させることで、コンテンツ鍵を保護する方法が開示されている。

特許文献1:特開2000-100069号公報

発明の開示

発明が解決しようとする課題

- [0004] この場合、コンテンツ鍵は外部に露見しないように厳重に管理される必要があるが、何らかの事故や事件により、不正者にコンテンツ鍵が暴露されることがあるかもしれない。一旦、コンテンツ鍵が不正者に暴露されてしまうと、それ以降のコンテンツについても同じ方法で、コンテンツ鍵を暴露されてしまう恐れがある。これにより、以降のコン

WO 2006/051791

2

PCT/JP2005/020470

テンツの不正利用を防ぐことができないことが想定される。従来技術では、規定の方法で保護されたコンテンツ鍵によってのみ、コンテンツデータが保護されていたため、この種の攻撃に対して、脆弱である。

[0005] 本発明は、上記の問題点に鑑み、何らかの事故や事件により、一旦コンテンツ保護を破る方法が発見されたとしても、他のコンテンツに対し、同じ方法でコンテンツを不正に利用することができないようなデータ再生方法及びデータ処理装置を提供することを目的とする。

課題を解決するための手段

[0006] 上記の目的を達成するために、本発明は、原デジタルデータが変形及び暗号化されて生成された保護化デジタルデータと、変形されたデジタルデータの復元において用いられる復元用情報が変形されて生成された変形復元用情報とが記録されている記録媒体から前記保護化デジタルデータを読み出し、再生するデータ再生方法であって、前記記録媒体から前記保護化デジタルデータを読み出し、読み出した前記保護化デジタルデータに、前記暗号化に対応する復号を施して、変形デジタルデータを生成する第1のステップと、前記復元用情報に基づいて、生成された前記変形デジタルデータに、前記変形に対応する復元を施して、復元デジタルデータを生成する第2のステップと、生成された前記復元デジタルデータを再生する第3のステップと、前記記録媒体から前記変形復元用情報を読み出し、読み出した前記変形復元用情報を用いて、前記第2のステップの処理が実行可能となる形式の前記復元用情報を生成する第4のステップと、前記第1のステップの前に、前記第4のステップを実行するように制御する制御ステップとを含むことを特徴とする。

[0007] ここで、前記第4のステップにおいて、前記復元用情報の生成を前記復元デジタルデータの再生の前に実行し、前記復元デジタルデータの再生中に、前記第1、第2及び第3のステップを並行して実行するとしてもよい。

ここで、前記復元用情報の変形は、ソフトウェア的に耐タンパ化することであるとしてもよい。

[0008] ここで、前記デジタルデータは、複数のコンテンツから構成され、前記復元用情報は、コンテンツ毎に、その実行処理の内容が異なるとしてもよい。

WO 2006/051791

3

PCT/JP2005/020470

ここで、前記保護化デジタルデータは、原デジタルデータが暗号化され、さらに変形されて生成されており、前記第1のステップにおいて、前記復号の代わりに、前記復元用情報に基づいて、読み出した前記保護化デジタルデータに、前記変形に対応する復元を施して、暗号化デジタルデータを生成し、前記第2のステップにおいて、前記復元の代わりに、前記暗号化デジタルデータに、前記暗号化に対応する復号を施して、前記復元デジタルデータを生成するとしてもよい。

[0009] また、本発明は、原デジタルデータが変形及び暗号化されて生成された保護化デジタルデータと、変形されたデジタルデータの復元において用いられる復元用情報に変形されて生成された変形復元用情報とが記録されている記録媒体から前記保護化デジタルデータを読み出し、再生するデータ再生方法であって、前記記録媒体から前記保護化デジタルデータを読み出し、読み出した前記保護化デジタルデータに、前記暗号化に対応する復号を施して、変形デジタルデータを生成する第1のステップと、前記復元用情報に基づいて、生成された前記変形デジタルデータに、前記変形に対応する復元を施して、復元デジタルデータを生成する第2のステップと、生成された前記復元デジタルデータを再生する第3のステップと、前記第1のステップの前に、前記記録媒体から前記変形復元用情報を読み出し、読み出した前記変形復元用情報に、前記変形に対応する復元を施して、変形前の前記復元用情報を生成する第4のステップとを含むことを特徴とする。

[0010] また、本発明は、原デジタルデータが変形及び暗号化されて生成された保護化デジタルデータと、変形されたデジタルデータの復元において用いられる復元用情報に変形されて生成された変形復元用情報とが記録されている記録媒体から前記保護化デジタルデータを読み出し、再生するデータ処理装置であって、前記記録媒体から前記保護化デジタルデータ及び変形復元用情報を読み出す読出手段と、読み出した前記保護化デジタルデータに、前記暗号化に対応する復号を施して、変形デジタルデータを生成する復号手段と、前記復元用情報に基づいて、生成された前記変形デジタルデータに、前記変形に対応する復元を施して、復元デジタルデータを生成する復元手段と、生成された前記復元デジタルデータを再生する再生手段と、前記記録媒体から前記変形復元用情報を読み出し、読み出した前記変形復元用情報

WO 2006/051791

4

PCT/JP2005/020470

報を用いて、前記復元手段の処理が実行可能となる形式の前記復元用情報を生成する生成手段と、前記復号手段による復号の前に、前記生成手段による前記復元用情報の生成を行うように制御する制御手段とを含むことを特徴とする。

- [0011] ここで、前記制御手段は、前記復元用情報の生成を前記復元デジタルデータの再生の前に実行し、前記復元デジタルデータの再生中に、前記復号手段、前記復元手段及び前記再生手段による復号、復元及び再生を並行して実行するとしてもよい。

ここで、前記復元用情報の変形は、ソフトウェア的に耐タンパ化することであるとしてもよい。

- [0012] ここで、前記デジタルデータは、複数のコンテンツから構成され、前記復元用情報は、コンテンツ毎に、その実行処理の内容が異なるとしてもよい。

ここで、前記保護化デジタルデータは、原デジタルデータが暗号化され、さらに変形されて生成されており、前記復号手段において、前記復号の代わりに、前記復元用情報に基づいて、読み出した前記保護化デジタルデータに、前記変形に対応する復元を施して、暗号化デジタルデータを生成し、前記復元手段において、前記復元の代わりに、前記暗号化デジタルデータに、前記暗号化に対応する復号を施して、前記復元デジタルデータを生成するとしてもよい。

- [0013] ここで、原デジタルデータが変形及び暗号化されて生成された保護化デジタルデータと、変形されたデジタルデータの復元において用いられる復元用情報が変形されて生成された変形復元用情報とが記録されている記録媒体から前記保護化デジタルデータを読み出し、再生するデータ処理装置であって、前記記録媒体から前記保護化デジタルデータ及び変形復元用情報を読み出す読出手段と、読み出した前記保護化デジタルデータに、前記暗号化に対応する復号を施して、変形デジタルデータを生成する復号手段と、前記復元用情報に基づいて、生成された前記変形デジタルデータに、前記変形に対応する復元を施して、復元デジタルデータを生成する復元手段と、生成された前記復元デジタルデータを再生する再生手段と、前記記録媒体から前記変形復元用情報を読み出し、読み出した前記変形復元用情報に、前記変形に対応する復元を施して、変形前の前記復元用情報を生成する生成手段と、

WO 2006/051791

5

PCT/JP2005/020470

前記復号手段による復号の前に、前記生成手段による前記復元用情報の生成を行うように制御する制御手段とを含むことを特徴とする。

発明の効果

[0014] 以上説明した発明によると、演算等と暗号化による二重の保護を行っているが、この意義は、次の通りである。

暗号化については統一方式を採用し、復元用情報等を用いた復元処理等をコンテンツ毎に異ならせた場合、仮に暗号化が不正に破られた場合でも、他のコンテンツについては、復元用情報等を用いた変換により保護されることとなる。これにより、コンテンツ等の著作権をより強固に保護することができる。

[0015] また、本発明によると、復元用情報の変換を、復号の前に実行しているが、その意義は次の通りである。

復元用情報の変換処理が、処理に時間の係る耐タンパ化されたプログラムの実行等を伴う場合などに有効である。つまり、復号処理以降の各処理の合間に復元用情報の変換処理を行った場合、その変換処理にかかる時間の分だけ他の処理が遅延するため、コンテンツの再生が途切れてしまう可能性があるが、復号処理以降の処理に移る前に予め復元用情報の変換処理を行っておくことにより、このような問題の発生を防ぐことができる。

[0016] なお、復元用情報とは、例えば、バイトコード、プログラム、固定長のバイト値等を示している。

図面の簡単な説明

[0017] [図1]本発明の実施の形態における、記録媒体及びコンテンツ再生装置の構成を示す図

[図2]本発明の実施の形態における、コンテンツ再生処理のフロー図

[図3]本発明の実施の形態における、コンテンツ再生装置の無効化確認処理のフロー図

[図4]本発明の実施の形態における、TRS化バイトコード処理のフロー図

[図5]本発明の実施の形態における、TRS化バイトコードのデータ構造

[図6]本発明の実施の形態における、保護コンテンツデータの復号処理のフロー図

WO 2006/051791

6

PCT/JP2005/020470

[図7]本発明の実施の形態における、変形コンテンツデータの復元処理例

[図8]本発明の実施の形態における、自己書き換えによるTRS化バイトコードからの復元用バイトコードの生成例

[図9]本発明の実施の形態における、TSデータの再生順序の入れ替えによる保護されたコンテンツの復元処理例

符号の説明

- [0018]
- 101 記録媒体
 - 102 コンテンツ再生装置
 - 111 再生制御情報
 - 112 TRS化バイトコード
 - 113 保護コンテンツデータ
 - 114 暗号化コンテンツ鍵
 - 115 無効化情報
 - 121 ディスク読込部
 - 122 再生制御部
 - 123 ユーザ操作受付部
 - 124 TRS化バイトコード実行部
 - 125 復号部
 - 126 コンテンツデータ復元処理部
 - 127 デコーダ
 - 128 コンテンツ鍵生成部
 - 129 無効化情報処理部
 - 130 デバイス鍵保持部
 - 501 暗号鍵用TRS化バイトコード
 - 502 暗号化された復元用バイトコード
 - 701 変形コンテンツデータの変形単位のビット列
 - 702 XOR演算に用いるパラメータ
 - 703 復元後の変形単位のビット列

WO 2006/051791

7

PCT/JP2005/020470

801 実行前コード

802 実行後コード

803 復元用バイトコード

901 復号部125での読込み順序

902 デコーダ127での読込み順序

発明を実施するための最良の形態

[0019] 以下、発明を実施するための最良の形態を、図面を参照しながら説明する。

本発明に用いる記録媒体には、コンテンツ鍵による暗号化と、暗号化とは別の演算によるデータ変形により、保護されているコンテンツデータを記録する。さらに、前記コンテンツ鍵と、前記演算の逆演算を実行するプログラムの両方を、保護した上で前記コンテンツデータと共に記録する。さらに、前記コンテンツ鍵が、前記コンテンツデータの利用が許可された正規のデータ処理装置のみが利用可能となる無効化情報により保護されており、前記無効化情報を併せて記録する。さらに、前記プログラムがTRS化(ソフトウェア的に耐タンパ化する処理)により保護されている。

[0020] また、コンテンツデータの記録手順は、前記コンテンツデータをコンテンツ鍵により暗号化するステップと、暗号化とは別の演算によりデータ変形するステップとを含む。さらに、前記コンテンツ鍵を保護した上で前記記録媒体に記録するステップと、前記演算の逆演算を実行するプログラムを前記コンテンツ鍵の保護方法とは異なる方法で保護した上で前記記録媒体に記録するステップとを含む。さらに、前記コンテンツ鍵を、前記コンテンツデータの利用が許可された正規のデータ処理装置のみを利用可能とする無効化情報により保護するステップを含む。さらに、前記プログラムをTRS化して保護するステップを含む。

[0021] 図1は、本発明の一実施形態に係る記録媒体、及びコンテンツ再生装置の構成を示す図である。

記録媒体101には、再生制御情報111、TRS (Tamper Resistant Software) 化バイトコード112、保護コンテンツデータ113、暗号化コンテンツ鍵114、無効化情報115が記録されている。記録媒体101は例えばBD (Blu-ray Disc)を想定しているが、それに限るものではない。

[0022] 本実施の形態では、1つのコンテンツは、複数のMPEG2-TS (Motion Picture Expert Group2-Transport Stream) データから構成されていることを想定している。コンテンツを再生する際の、データの再生順序を規定しているのが、再生制御情報111である。

TRS化バイトコード112(変形復元用情報の一例)は、解析行為によりソフトウェアに含まれる秘密情報や処理内容を把握されないための処理が施されたバイトコード(復元用情報の一例)である。バイトコードの具体的な実行内容については後述する。なお、本実施の形態では、バイトコードとしているが、バイトコード以外の実行プログラムでも構わない。

[0023] 保護コンテンツデータ113(保護化デジタルデータの一例)は、デコーダによって映像を出力できる平文MPEG2-TSデータ(デジタルデータの一例)に対し、コンテンツ鍵による暗号処理、及び、ある値とのXOR演算する等の変形処理が施されたデータである。

暗号化コンテンツ鍵114は、コンテンツデータを復号するためのコンテンツ鍵をメディア鍵にて暗号化したデータである。

[0024] 無効化情報115について説明する。鍵管理機関は、複数のデバイス鍵及び複数のメディア鍵からなる集合を有している。鍵管理機関は、コンテンツ再生装置102の各々に、1個のデバイス鍵、及びそのデバイス鍵の鍵識別番号を割り当て、割り当てたデバイス鍵、及び鍵識別番号をコンテンツ再生装置102に与える。また、記録媒体101に1個のメディア鍵を割り当てる。次に、鍵管理機関は、コンテンツ再生装置102の各々に割り当てられた各デバイス鍵を用いてメディア鍵を暗号化して暗号化メディア鍵を作成し、全てのデバイス鍵に対する暗号化メディア鍵と鍵識別番号からなるリストを作成する。このリストが無効化情報115である。なお、この単純な方法では、コンテンツ再生装置102の台数が大量になると無効化情報115のデータサイズが非現実的な大きな値になるという欠点があるため、「デジタルコンテンツ保護用鍵管理方式」(中野、大森、館林、2001年 暗号と情報セキュリティシンポジウム、SCIS2001 5 A-5, Jan. 2001)で開示されている無効化情報115のデータサイズを圧縮する方法を用いても構わない。また、この方法に限らず、無効化情報115のデータサイズを

WO 2006/051791

9

PCT/JP2005/020470

圧縮する他の方法を用いても構わない。

[0025] コンテンツ再生装置102は、ディスク読込部121、再生制御部122、ユーザ操作受付部123、TRS化バイトコード実行部124、復号部125、コンテンツデータ復元処理部126、デコーダ127、コンテンツ鍵生成部128、無効化情報処理部129、デバイス鍵保持部130から構成される。それぞれの一実施例としては、ディスク読込部121はBDドライブであり、その他はCPU、ワークメモリ、HDDなどから構成されるPCでの実現を想定しているが、それに限るものではない。

[0026] 以上で、本発明の一実施形態に係る記録媒体101、及びコンテンツ再生装置102の構成に関する説明を終了する。

(コンテンツ再生処理の説明)

図2を用いて、コンテンツ再生処理について説明する。

まず、ユーザ操作受付部123でユーザからのコンテンツ再生開始要求を受付けた時点から、コンテンツ再生処理が開始される。

[0027] コンテンツ再生要求を受付けたら、無効化情報処理部129がコンテンツ再生装置102の無効化確認処理を行う(S201)。無効化確認処理の詳細については、後述する。

以降、無効化確認処理S201でのメディア鍵の生成の成否により処理が分岐する(S202)。

無効化確認処理S201でメディア鍵の生成に成功した場合、再生制御部122が保護コンテンツデータ113の選択を行う(S203)。

[0028] 無効化確認処理S201でメディア鍵の生成に失敗した場合、コンテンツ再生装置102が無効化されていることを通知し処理を終了する(S208)。

S203の処理が終了後、選択した保護コンテンツデータ113の再生に必要なTRS化バイトコード112を読み出し、TRS化バイトコード実行部124にて、TRS化バイトコード実行処理を行う(S204)。TRS化バイトコード実行処理の詳細については、後述する。なお、ここまでの処理が、コンテンツが表示されるまでに行われる前処理となる。

[0029] 再生制御部122は、再生制御情報111に従って、保護コンテンツデータ113の読

WO 2006/051791

10

PCT/JP2005/020470

み出しを指示する。コンテンツ鍵生成部128、及び復号部125によって、読み出された保護コンテンツデータ113の復号が行われる(S205)。以降、保護コンテンツデータ113を復号した結果を、変形コンテンツデータ(変形デジタルデータの一例)と呼ぶ。保護コンテンツの暗号化には、AES(Advanced Encryption Standard)が用いられるが、これに限定されるものではない。コンテンツ再生中は、保護コンテンツデータ113の終了まで繰り返し復号処理が行われるため、後述の変形コンテンツの復元(S206)、コンテンツのデコード(S207)と並行して実行される。保護コンテンツデータ113の復号処理の詳細については、後述する。

[0030] 復号部125より出力される変形コンテンツデータに対し、コンテンツデータ復元処理部126は復元処理を行う(S206)。復元処理は、記録媒体101上での記録単位であるセクタ、もしくはMPEG2-TSデータにある、一定個数のMPEG2-TSパケットから構成されるAligned unitを単位として実行され、コンテンツ再生中は、保護コンテンツデータ113の復号処理(S205)、後述のコンテンツのデコード(S207)と並行して実行される。変形コンテンツデータの復元処理の詳細については、後述する。

[0031] 復元されたコンテンツデータは、デコーダ127にてデコードされ、例えばテレビモニター等の映像を表示する装置に出力される(S207)。コンテンツ再生中は、保護コンテンツデータ113の復号(S205)、変形コンテンツデータの復元(S206)と並行して実行される。

コンテンツデータを全て再生し終えた時点で、コンテンツ再生処理は終了する。

[0032] 以上で、コンテンツ再生処理の説明を終了する。

(コンテンツ再生装置102の無効化確認処理)

図3を用いて、コンテンツ再生装置102の無効化確認処理を説明する。

無効化確認処理とは、図2でのコンテンツ再生開始後に、コンテンツ再生装置102が記録媒体101に記録された無効化情報115によって、無効化されていないかを確認する処理(S201に相当)である。

[0033] 無効化情報処理部129は、デバイス鍵保持部130から取得したデバイス鍵を読み込む(S301)。デバイス鍵は、コンテンツ再生装置102を特定することのできる情報であり、コンテンツ再生装置102毎に固有である。

WO 2006/051791

11

PCT/JP2005/020470

次に、記録媒体101に記録されている無効化情報115を読み込む(S302)。読み込んだデバイス鍵と無効化情報115を用いて、メディア鍵を生成する(S303)。

- [0034] コンテンツ再生装置102が無効化されている場合には、メディア鍵は生成できない。デバイス鍵と無効化情報115を用いたメディア鍵の生成については、「National Technical Report 第43巻第3号p. 118～p. 122」(松下電器産業株式会社技術総務センター平成9年6月18日発行)に詳しい。

以上で、コンテンツ再生装置102の無効化確認処理の説明を終了する。

- [0035] (TRS化バイトコード実行処理)

図4を用いて、TRS化バイトコード実行処理(図2のS204に相当)について説明する。

TRS化バイトコード実行部124は、指示されたコンテンツの再生に必要なTRS化バイトコード112を記録媒体101から取得する(S401)。

- [0036] 取得したTRS化バイトコード112をTRS化バイトコード実行部124で実行することにより、復元用バイトコードを出力する(S402)。復元用バイトコードとは、コンテンツデータ復元処理部126にて実行できるバイトコードである。

図7を用いて、コンテンツ復元処理部126での変形コンテンツデータの復元処理S206の具体例を説明する。図7では、復元用バイトコードを実行することにより、変形コンテンツデータに対し、或る値とのXOR演算を行ってコンテンツデータを復元するバイトコードの処理について説明する。701は、変形コンテンツデータの変形単位のビット列を表している。パラメータ702は、変形コンテンツデータを復元するためにXOR演算するためのパラメータを示している。パラメータ702は、復元用バイトコード内で規定されている。コンテンツ復元処理部126は、復元用バイトコードを実行することにより、変形コンテンツデータの変形単位701とパラメータ702をXORした結果を平文コンテンツデータ703として出力する。上記の処理を繰り返し実行することで、変形コンテンツデータ全体を復元する。

- [0037] その実行処理は、「バイトコード内の特定のバイト列」の他に、「復元対象となる処理単位内データの特定番地にある値」やこれらを組み合わせた値と、変形コンテンツデータのXORを演算することを想定しているが、これに限るものでない。XORの他に、

WO 2006/051791

12

PCT/JP2005/020470

ROT等の処理負荷が小さい演算を幾つか組み合わせたものであっても構わない。
復元用バイトコードは、コンテンツ毎に、その実行処理が異なっても構わない。

[0038] また、TRS化バイトコード112は、図5のように、暗号鍵用TRS化バイトコード501と暗号化された復元用バイトコード502(変形復元用情報の一例)を結合したデータであつてもよい。この場合、暗号鍵用TRS化バイトコード501はTRS化バイトコード実行部124で実行することにより、暗号化された復元用バイトコード502の暗号鍵を出力する。出力された暗号鍵と暗号化された復元用バイトコード502を復号部125に送信し、復元用バイトコードを生成する。生成された復元用バイトコードは、コンテンツ復元部126に送信され、処理を継続する。

[0039] さらに、上記の例では、記録媒体101に記録されたTRS化バイトコード112とは別の復元用バイトコードを出力したが、TRS化バイトコード実行処理S204により、TRS化バイトコード112の一部のコードを自己書き換えして生成した、復元用バイトコードを出力してもよい。図8を用いて、自己書き換えして復元用バイトコード803を生成するTRS化バイトコード実行処理S204について説明する。図8では、TRS化バイトコード112の実行前コード801を、TRS化バイトコード実行処理S204により、実行後コード802に自己書き換えして復元用バイトコード803を出力する。また、復元用バイトコード803をコンテンツ復元処理部126で実行する場合は、TRS化バイトコード実行処理S204で書き換えられた実行後コード802が再度書き換えられることはない。また、コンテンツ再生中は、図2における保護コンテンツデータ113の復号S205、変形コンテンツデータの復元S206と並行して実行でき、且つ表示される映像が乱れることがない。

[0040] (保護コンテンツデータ113の復号処理)

図6を用いて、保護コンテンツデータ113の復号処理(図2のS205に相当)について説明する。

コンテンツ鍵生成部128は、ディスク読込部121を介して、暗号化コンテンツ鍵114を記録媒体101より取得する(S601)。

[0041] 次に、コンテンツ鍵生成部128は、図2における、コンテンツ再生装置102の無効化確認処理S201にて生成したメディア鍵を無効化情報処理部129から取得し、暗

WO 2006/051791

13

PCT/JP2005/020470

号化コンテンツ鍵114を復号する(S602)。

復号部125は、ディスク読込部121を介して、保護コンテンツデータ113を記録媒体101より取得する(S603)。

[0042] 復号部125は、コンテンツ鍵生成部128よりコンテンツ鍵を取得し、保護コンテンツデータ113を復号する(S604)。復号結果として出力される変形コンテンツデータは、コンテンツ復元処理部126へ送信される。

以上で、保護コンテンツデータ113の復号処理について説明を終了する。

なお、本実施の形態では、保護コンテンツデータ113は、平文コンテンツデータに対して、変形処理が為された後、暗号化されているが、暗号化された後、変形処理が為されてもよい。この場合、図2においてS205とS206の処理順序が入れ替わる。

[0043] また、本実施の形態では、図2のTRS化バイトコード実行処理S204において、復元用バイトコードを出力したが、TRS化バイトコード実行処理S204の出力として、固定長のバイト値(復元用情報の一例)が出力されても構わない。この場合、変形コンテンツデータの復元処理S206は、TRS化バイトコード実行処理S204によって出力された値を用いて、例えば「変形コンテンツデータと、S204の出力値とのXOR演算をする」等、演算処理自体は固定されている。

[0044] また、本実施の形態では、図2の変形コンテンツの復元S206において、変形コンテンツデータに対し、XOR等の演算処理を行うこととしているが、コンテンツを構成するMPEG2-TSファイルの読込み順序と、再生順序を変更させることで、コンテンツを保護しても構わない。図9を用いて、上記の処理について説明する。再生制御情報111は、コンテンツが4つのTSファイルa～dで構成され、復号部125での読込み順序901として、TSデータb→TSデータa→TSデータd→TSデータcの順で読込むことを表している。図2において、再生制御情報111に従って各々のTSデータに対応する保護コンテンツデータ113を読み込み、保護コンテンツデータ113の復号S205を行う。続いて、S206で復元用バイトコードを実行することにより、予め指示されているデコーダ127での読込み順序902に従って、復号されたTSデータをTSデータa→TSデータb→TSデータc→TSデータdの順に入れ替えてデコーダ127へ出力する。この場合、再生制御情報111で指示されている再生順序に従って再生したとしても、

WO 2006/051791

14

PCT/JP2005/020470

正しい順序では再生されない。さらに、各TSデータの再生時間が十分短くした場合、コンテンツ内のシーンから、コンテンツの正規の再生順序を推測することはできない。このように、復元用バイトコードを用いて、コンテンツを構成するMPEG2-TSデータの読み込み順序と、デコーダ127への読み込み順序を変更させることで、コンテンツを保護しても構わない。

[0045] (まとめ)

(1) 本実施の形態では、上述したように、1つのコンテンツは、所定数のMPEG2-TSデータから構成されていると想定している。

記録媒体101は、1個の再生制御情報と、前記所定数と同数のTRS化バイトコードと、前記所定数と同数の保護コンテンツデータと、前記所定数と同数の暗号化コンテンツ鍵と、1個の無効化情報を格納しており、前記再生制御情報と、所定数のTRS化バイトコードと、前記所定数の保護コンテンツデータと、前記所定数の暗号化コンテンツ鍵とは、前記コンテンツを構成している。

[0046] 前記所定数の保護コンテンツデータのそれぞれは、前記所定数のTRS化バイトコードのそれぞれに対応しており、また、前記所定数の暗号化コンテンツ鍵のそれぞれに対応している。

(2) 保護コンテンツデータ113は、コンテンツ配信装置により、例えば、次のようにして生成される。

[0047] 1個のMPEG2-TSデータの少なくとも一部分について、その一部分とある値とにXOR演算を施し、得られた演算結果を、前記一部分と置き換える。その後、コンテンツ鍵を用いて、例えば、AESによる暗号化アルゴリズムを施して保護コンテンツデータ113を生成する。

(3) 無効化情報115は、複数の暗号化メディア鍵を含んでいる。複数の暗号化メディア鍵は、それぞれ、複数のデバイスに対応しており、例えば、各デバイスのデバイス識別子が付加されている。ここで、デバイスは、例えば、コンテンツ再生装置である。

[0048] 鍵管理機関が有する鍵管理サーバ装置は、無効化されていないデバイスについて、当該デバイスに割り当てられたデバイス鍵を用いて、メディア鍵を暗号化して暗号化メディア鍵を生成する。無効化されているデバイスについては、当該デバイスに割

WO 2006/051791

15

PCT/JP2005/020470

り当てられたデバイス鍵を用いて、所定の検知情報を暗号化して暗号化メディア鍵を生成する。ここで、所定の検知情報は、固定値であり、例えば、値「0」である。

[0049] 無効化情報処理部129は、無効化情報115から、コンテンツ再生装置102に対応する暗号化メディア鍵を選択し、選択した暗号化メディア鍵を、デバイス鍵保持部130から取得したデバイス鍵を用いて、復号して復号情報を得る。ここで、得られた復号情報が、「0」であれば、コンテンツ再生装置102は、無効化されているとみなされ、またメディア鍵の生成に失敗したとみなされる。得られた復号情報が、「0」でなければ、コンテンツ再生装置102は、無効化されておらず、メディア鍵の生成に成功し、得られた復号情報は、メディア鍵であるとみなされる。

[0050] (4)TRS化バイトコード実行処理は、ローテーション演算であるROTでもよい。ローテーション演算の一例は、次の通りである。

例えば、ROT2(X)は、32ビットのデータXを左へ2ビット循環シフトすることを示す。32ビットのデータXを左へ2ビット循環シフトするとは、データXを最上位2ビットX1と最下位30ビットX2に分け、X2を、データXの最上位30ビットにシフトし、X1をデータXの最下位2ビットにシフトすることを言う。

[0051] (5)図8に示すTRS化バイトコード112は、例えば、所定の平文データが暗号化された暗号化データと、この暗号化データを復号する復号用のコンピュータプログラムと、復号により得られた平文データにより、実行前コード801を自己書き換えする書き換え用のコンピュータプログラムを含んでいる。

TRS化バイトコード112が実行されると、TRS化バイトコード112に含まれる前記暗号化データが、前記復号用のコンピュータプログラムにより復号されて平文データが生成され、前記書き換え用のコンピュータプログラムが、TRS化バイトコード112の一部分である実行前コード801に、生成した平文データを上書きする。こうして、上書きされた部分である実行後コード802を含む復元用バイトコード803が生成される。

[0052] (6)図9に示すTSデータの入れ換えが行われる場合に、復元用バイトコードは、例えば、次のような2個の命令を含む。

「SWAP TSデータb、TSデータa」 (命令1)

「SWAP TSデータd、TSデータc」 (命令2)

WO 2006/051791

16

PCT/JP2005/020470

ここで、命令「SWAP A、B」は、TSデータである「A」と「B」の再生順序を入れ替えることを示している。命令「SWAP A、B」が実行されると、最初にTSデータ「B」が再生され、次に、TSデータ「A」が再生されるように、再生順序が入れ替えられることを示している。

[0053] 上記の命令1及び命令2が実行されると、各TSデータの再生順序は、上述したように、TSデータa→TSデータb→TSデータc→TSデータdとなる。

(その他の変形例)

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

[0054] (1)上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。ここで、コンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わされて構成されたものである。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。つまり、前記マイクロプロセッサは、前記コンピュータプログラムに含まれる各命令を1個ずつ読み出し、読み出した命令を解釈し、解釈結果に従って動作する。

[0055] (2)上記の各装置を構成する構成要素の一部又は全部は、1個のシステムLSI(Large Scale Integration:大規模集積回路)から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。

[0056] また、上記の各装置を構成する構成要素の各部は、個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されてもよい。また、ここでは、LSIとしたが、

WO 2006/051791

17

PCT/JP2005/020470

集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)やLSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用しても良い。

[0057] (3) 上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なICカード又は単体のモジュールから構成されているとしてもよい。前記ICカード又は前記モジュールは、マイクロプロセッサ、ROM、RAM、などから構成されるコンピュータシステムである。前記ICカード又は前記モジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記ICカード又は前記モジュールは、その機能を達成する。このICカード又はこのモジュールは、耐タンパ性を有するとしてもよい。

[0058] (4) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0059] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0060] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送する

WO 2006/051791

18

PCT/JP2005/020470

ことにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(5) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0061] 本発明にかかる、著作権を保護するために暗号化及び変形されたコンテンツデータと、それを再生するために必要な情報を記録した情報記録媒体、データ処理方法、及びデータ処理装置は、パッケージメディア等の分野において有用である。

また、本発明を構成する各装置及び記録媒体は、著作権の保護を要するコンテンツを制作し、配給するコンテンツ配給産業において、経営的に、また継続的及び反復的に使用することができる。また、本発明を構成する各装置及び記録媒体は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。

WO 2006/051791

19

PCT/JP2005/020470

請求の範囲

- [1] 原デジタルデータが変形及び暗号化されて生成された保護化デジタルデータと、変形されたデジタルデータの復元において用いられる復元用情報が変形されて生成された変形復元用情報とが記録されている記録媒体から前記保護化デジタルデータを読み出し、再生するデータ再生方法であって、
- 前記記録媒体から前記保護化デジタルデータを読み出し、読み出した前記保護化デジタルデータに、前記暗号化に対応する復号を施して、変形デジタルデータを生成する第1のステップと、
- 前記復元用情報に基づいて、生成された前記変形デジタルデータに、前記変形に対応する復元を施して、復元デジタルデータを生成する第2のステップと、
- 生成された前記復元デジタルデータを再生する第3のステップと、
- 前記記録媒体から前記変形復元用情報を読み出し、読み出した前記変形復元用情報を用いて、前記第2のステップの処理が実行可能となる形式の前記復元用情報を生成する第4のステップと、
- 前記第1のステップの前に、前記第4のステップを実行するように制御する制御ステップと
- を含むことを特徴とするデータ再生方法。
- [2] 前記第4のステップにおいて、前記復元用情報の生成を前記復元デジタルデータの再生の前に実行し、前記復元デジタルデータの再生中に、前記第1、第2及び第3のステップを並行して実行すること
- ことを特徴とする請求項1に記載のデータ再生方法。
- [3] 前記復元用情報の変形は、ソフトウェア的に耐タンパ化することであることを特徴とする請求項1に記載のデータ再生方法。
- [4] 前記デジタルデータは、複数のコンテンツから構成され、
- 前記復元用情報は、コンテンツ毎に、その実行処理の内容が異なる
- ことを特徴とする請求項1に記載のデータ再生方法。
- [5] 前記保護化デジタルデータは、原デジタルデータが暗号化され、さらに変形されて生成されており、

WO 2006/051791

20

PCT/JP2005/020470

前記第1のステップにおいて、前記復号の代わりに、前記復元用情報に基づいて、読み出した前記保護化デジタルデータに、前記変形に対応する復元を施して、暗号化デジタルデータを生成し、

前記第2のステップにおいて、前記復元の代わりに、前記暗号化デジタルデータに、前記暗号化に対応する復号を施して、前記復元デジタルデータを生成する

ことを特徴とする請求項1～4のいずれかに記載のデータ再生方法。

- [6] 原デジタルデータが変形及び暗号化されて生成された保護化デジタルデータと、変形されたデジタルデータの復元において用いられる復元用情報が変形されて生成された変形復元用情報とが記録されている記録媒体から前記保護化デジタルデータを読み出し、再生するデータ再生方法であって、

前記記録媒体から前記保護化デジタルデータを読み出し、読み出した前記保護化デジタルデータに、前記暗号化に対応する復号を施して、変形デジタルデータを生成する第1のステップと、

前記復元用情報に基づいて、生成された前記変形デジタルデータに、前記変形に対応する復元を施して、復元デジタルデータを生成する第2のステップと、

生成された前記復元デジタルデータを再生する第3のステップと、

前記第1のステップの前に、前記記録媒体から前記変形復元用情報を読み出し、読み出した前記変形復元用情報に、前記変形に対応する復元を施して、変形前の前記復元用情報を生成する第4のステップと

を含むことを特徴とするデータ再生方法。

- [7] 原デジタルデータが変形及び暗号化されて生成された保護化デジタルデータと、変形されたデジタルデータの復元において用いられる復元用情報が変形されて生成された変形復元用情報とが記録されている記録媒体から前記保護化デジタルデータを読み出し、再生するデータ処理装置であって、

前記記録媒体から前記保護化デジタルデータ及び変形復元用情報を読み出す読出手段と、

読み出した前記保護化デジタルデータに、前記暗号化に対応する復号を施して、変形デジタルデータを生成する復号手段と、

WO 2006/051791

21

PCT/JP2005/020470

前記復元用情報に基づいて、生成された前記変形デジタルデータに、前記変形に対応する復元を施して、復元デジタルデータを生成する復元手段と、

生成された前記復元デジタルデータを再生する再生手段と、

前記記録媒体から前記変形復元用情報を読み出し、読み出した前記変形復元用情報を用いて、前記復元手段の処理が実行可能となる形式の前記復元用情報を生成する生成手段と、

前記復号手段による復号の前に、前記生成手段による前記復元用情報の生成を行うように制御する制御手段と

を含むことを特徴とするデータ処理装置。

- [8] 前記制御手段は、前記復元用情報の生成を前記復元デジタルデータの再生の前に実行し、前記復元デジタルデータの再生中に、前記復号手段、前記復元手段及び前記再生手段による復号、復元及び再生を並行して実行する

ことを特徴とする請求項7に記載のデータ処理装置。

- [9] 前記復元用情報の変形は、ソフトウェア的に耐タンパ化することであることを特徴とする請求項7に記載のデータ処理装置。

- [10] 前記デジタルデータは、複数のコンテンツから構成され、
前記復元用情報は、コンテンツ毎に、その実行処理の内容が異なる
ことを特徴とする請求項7に記載のデータ処理装置。

- [11] 前記保護化デジタルデータは、原デジタルデータが暗号化され、さらに変形されて生成されており、

前記復号手段において、前記復号の代わりに、前記復元用情報に基づいて、読み出した前記保護化デジタルデータに、前記変形に対応する復元を施して、暗号化デジタルデータを生成し、

前記復元手段において、前記復元の代わりに、前記暗号化デジタルデータに、前記暗号化に対応する復号を施して、前記復元デジタルデータを生成する

ことを特徴とする請求項7～10のいずれかに記載のデータ処理装置。

- [12] 原デジタルデータが変形及び暗号化されて生成された保護化デジタルデータと、
変形されたデジタルデータの復元において用いられる復元用情報が変形されて生成

WO 2006/051791

22

PCT/JP2005/020470

された変形復元用情報とが記録されている記録媒体から前記保護化デジタルデータを読み出し、再生するデータ処理装置であって、

前記記録媒体から前記保護化デジタルデータ及び変形復元用情報を読み出す読出手段と、

読み出した前記保護化デジタルデータに、前記暗号化に対応する復号を施して、変形デジタルデータを生成する復号手段と、

前記復元用情報に基づいて、生成された前記変形デジタルデータに、前記変形に対応する復元を施して、復元デジタルデータを生成する復元手段と、

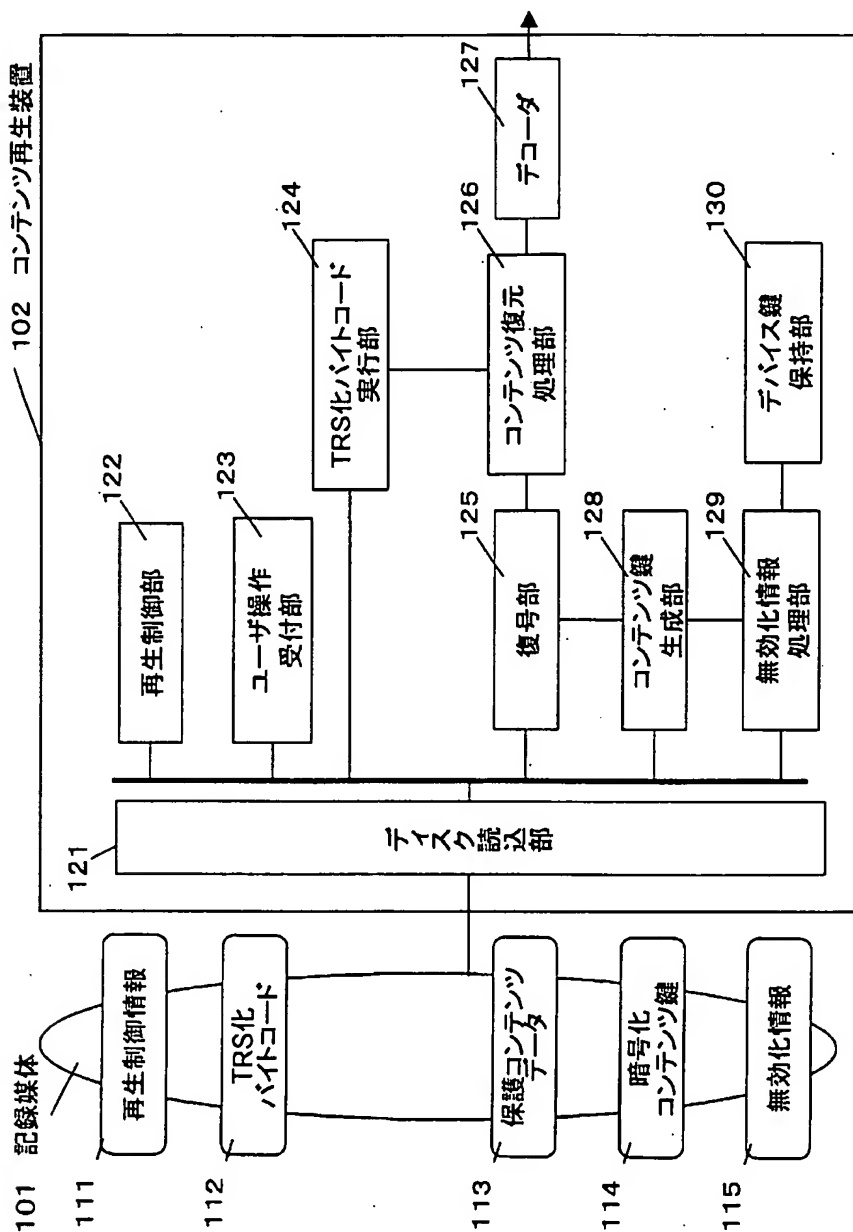
生成された前記復元デジタルデータを再生する再生手段と、

前記記録媒体から前記変形復元用情報を読み出し、読み出した前記変形復元用情報に、前記変形に対応する復元を施して、変形前の前記復元用情報を生成する生成手段と、

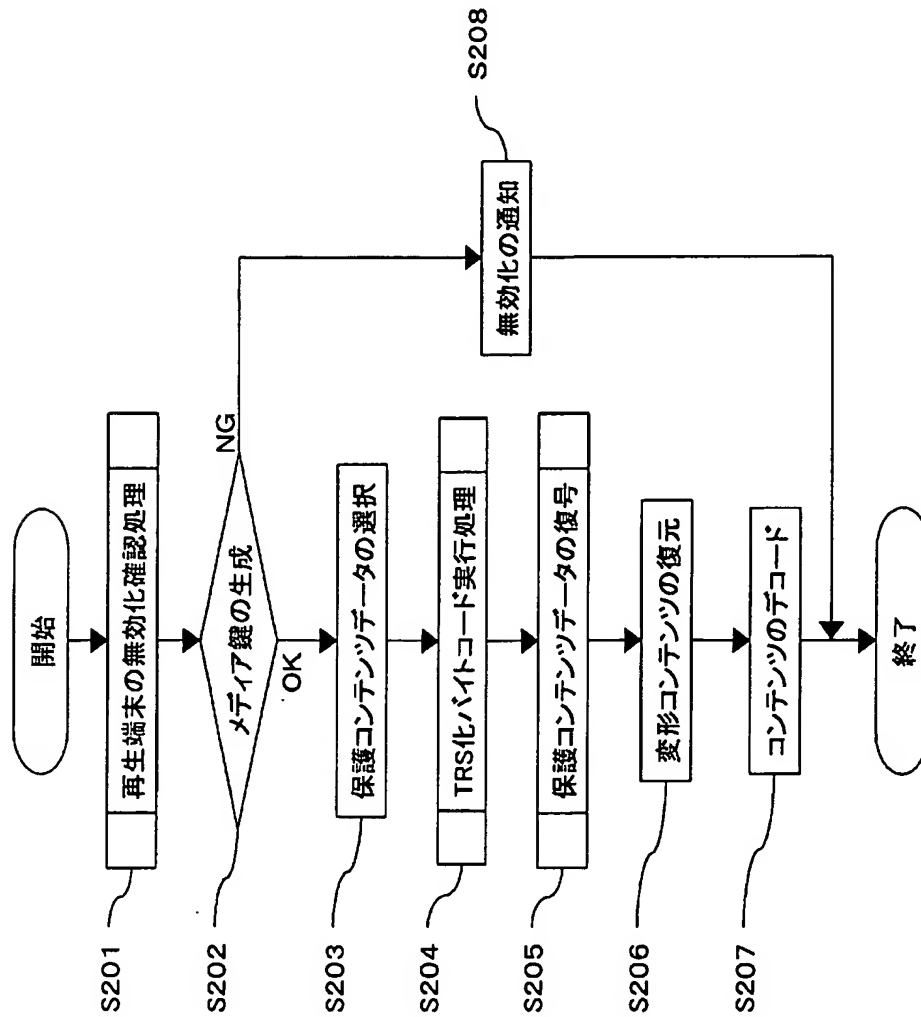
前記復号手段による復号の前に、前記生成手段による前記復元用情報の生成を行うように制御する制御手段と

を含むことを特徴とするデータ処理装置。

[図1]



[図2]

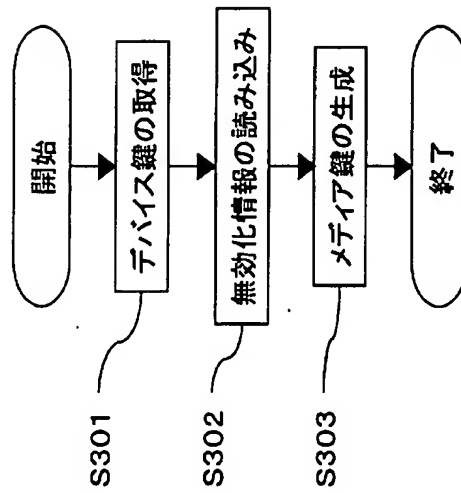


3/9

WO 2006/051791

PCT/JP2005/020470

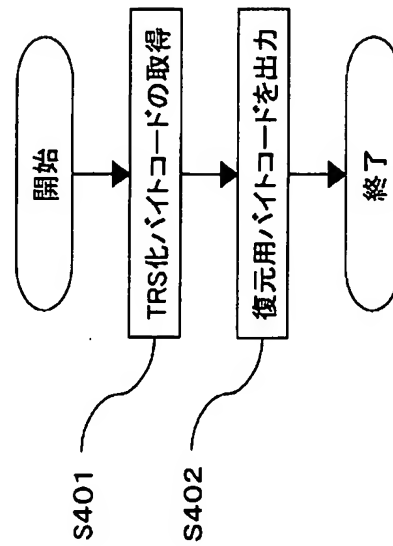
[図3]



WO 2006/051791

PCT/JP2005/020470

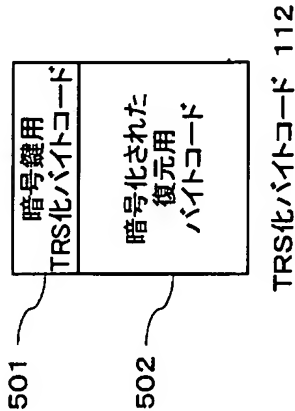
[図4]



WO 2006/051791

PCT/JP2005/020470

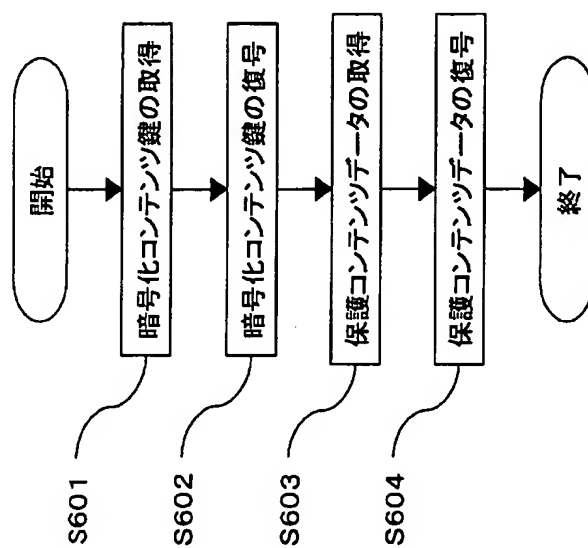
[図5]



WO 2006/051791

PCT/JP2005/020470

[図6]



7/9

WO 2006/051791

PCT/JP2005/020470

[図7]

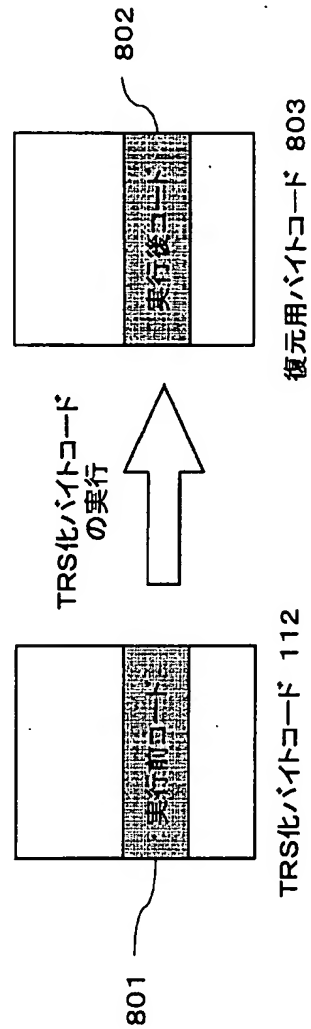
1010....	1010	—	701
xor 0000....	1111	—	702

1010....	0101	—	703

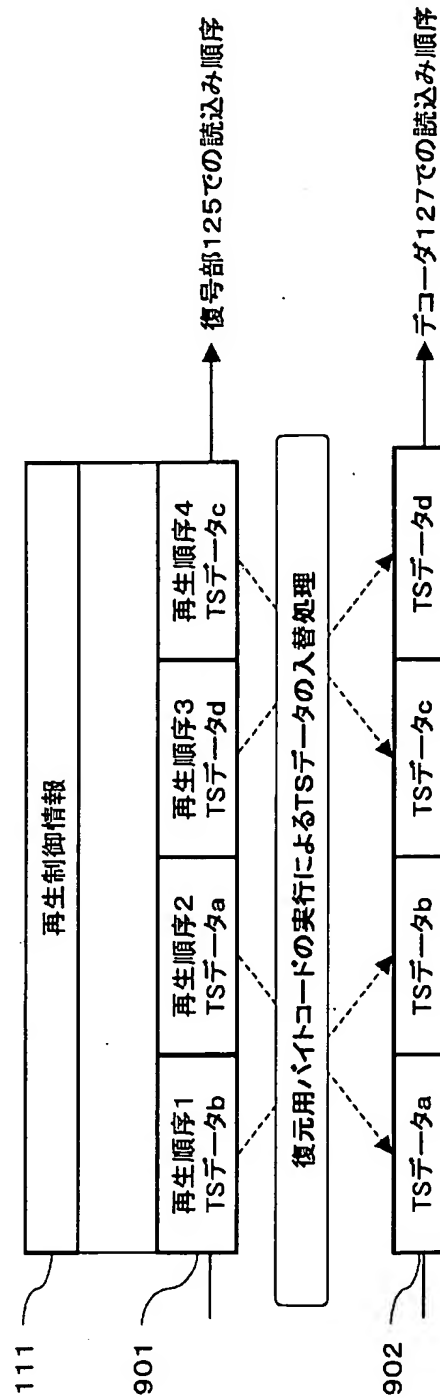
WO 2006/051791

PCT/JP2005/020470

[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/020470

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/24(2006.01), G09C1/00(2006.01), G10L19/00(2006.01), G11B20/10(2006.01), G11B27/00(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/24(2006.01), G09C1/00(2006.01), G10L19/00(2006.01), G11B20/10(2006.01), G11B27/00(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-113452 A (Sony Corp.), 21 April, 2000 (21.04.00), All pages; all drawings; particularly, Figs. 1, 4 & US 6665240 B1	1-12
Y	JP 9-134310 A (Fujitsu Ltd.), 20 May, 1997 (20.05.97), All pages; all drawings & US 2003/46564 A1	1-12
A	JP 2000-29792 A (Hitachi, Ltd.), 28 January, 2000 (28.01.00), All pages; all drawings (Family: none)	1-12

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
16 December, 2005 (16.12.05)

Date of mailing of the international search report
27 December, 2005 (27.12.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/020470

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 63-182758 A (NEC Corp.), 28 July, 1988 (28.07.88), All pages; all drawings (Family: none)	1-12
A	JP 3-233792 A (Nihon Denki Office System Kabushiki Kaisha), 17 October, 1991 (17.10.91), All pages; all drawings (Family: none)	1-12

国際調査報告		国際出願番号 PCT/J P 2 0 0 5 / 0 2 0 4 7 0													
<p>A. 発明の属する分野の分類 (国際特許分類 (IPC))</p> <p>Int.Cl. G06F21/24 (2006.01), G09C1/00 (2006.01), G10L19/00 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01)</p>															
<p>B. 調査を行った分野</p> <p>調査を行った最小限資料 (国際特許分類 (IPC))</p> <p>Int.Cl. G06F21/24 (2006.01), G09C1/00 (2006.01), G10L19/00 (2006.01), G11B20/10 (2006.01), G11B27/00 (2006.01)</p>															
<p>最小限資料以外の資料で調査を行った分野に含まれるもの</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">日本国実用新案公報</td> <td style="width: 50%;">1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2005年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2005年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2005年</td> </tr> </table>				日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2005年	日本国実用新案登録公報	1996-2005年	日本国登録実用新案公報	1994-2005年				
日本国実用新案公報	1922-1996年														
日本国公開実用新案公報	1971-2005年														
日本国実用新案登録公報	1996-2005年														
日本国登録実用新案公報	1994-2005年														
<p>国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)</p>															
<p>C. 関連すると認められる文献</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">引用文献の カテゴリー*</th> <th style="width: 70%;">引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示</th> <th style="width: 20%;">関連する 請求の範囲の番号</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Y</td> <td>JP 2000-113452 A (ソニー株式会社) 2000.04.21, 全頁, 全図, 特に【図1】及び【図4】 & US 6665240 B1</td> <td style="text-align: center;">1-12</td> </tr> <tr> <td style="text-align: center;">Y</td> <td>JP 9-134310 A (富士通株式会社) 1997.05.20, 全頁, 全図 & US 2003/46564 A1</td> <td style="text-align: center;">1-12</td> </tr> <tr> <td style="text-align: center;">A</td> <td>JP 2000-29792 A (株式会社日立製作所) 2000.01.28, 全頁, 全図 (ファミリーなし)</td> <td style="text-align: center;">1-12</td> </tr> </tbody> </table>				引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	Y	JP 2000-113452 A (ソニー株式会社) 2000.04.21, 全頁, 全図, 特に【図1】及び【図4】 & US 6665240 B1	1-12	Y	JP 9-134310 A (富士通株式会社) 1997.05.20, 全頁, 全図 & US 2003/46564 A1	1-12	A	JP 2000-29792 A (株式会社日立製作所) 2000.01.28, 全頁, 全図 (ファミリーなし)	1-12
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号													
Y	JP 2000-113452 A (ソニー株式会社) 2000.04.21, 全頁, 全図, 特に【図1】及び【図4】 & US 6665240 B1	1-12													
Y	JP 9-134310 A (富士通株式会社) 1997.05.20, 全頁, 全図 & US 2003/46564 A1	1-12													
A	JP 2000-29792 A (株式会社日立製作所) 2000.01.28, 全頁, 全図 (ファミリーなし)	1-12													
<p><input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。</p>															
<p>* 引用文献のカテゴリー</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <p>「A」 特に関連のある文献ではなく、一般的技術水準を示すもの</p> <p>「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの</p> <p>「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)</p> <p>「O」 口頭による開示、使用、展示等に言及する文献</p> <p>「P」 国際出願日前で、かつ優先権の主張の基礎となる出願</p> </td> <td style="width: 50%; vertical-align: top;"> <p>の日の後に公表された文献</p> <p>「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの</p> <p>「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの</p> <p>「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの</p> <p>「&」 同一パテントファミリー文献</p> </td> </tr> </table>				<p>「A」 特に関連のある文献ではなく、一般的技術水準を示すもの</p> <p>「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの</p> <p>「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)</p> <p>「O」 口頭による開示、使用、展示等に言及する文献</p> <p>「P」 国際出願日前で、かつ優先権の主張の基礎となる出願</p>	<p>の日の後に公表された文献</p> <p>「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの</p> <p>「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの</p> <p>「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの</p> <p>「&」 同一パテントファミリー文献</p>										
<p>「A」 特に関連のある文献ではなく、一般的技術水準を示すもの</p> <p>「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの</p> <p>「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)</p> <p>「O」 口頭による開示、使用、展示等に言及する文献</p> <p>「P」 国際出願日前で、かつ優先権の主張の基礎となる出願</p>	<p>の日の後に公表された文献</p> <p>「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの</p> <p>「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの</p> <p>「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの</p> <p>「&」 同一パテントファミリー文献</p>														
<p>国際調査を完了した日</p> <p style="text-align: center;">16.12.2005</p>		<p>国際調査報告の発送日</p> <p style="text-align: center;">27.12.2005</p>													
<p>国際調査機関の名称及びあて先</p> <p style="text-align: center;">日本国特許庁 (ISA/J P) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号</p>		<p>特許庁審査官 (権限のある職員)</p> <p style="text-align: center;">高橋 克</p> <p>電話番号 03-3581-1101 内線 3546</p>													

国際調査報告

国際出願番号 PCT/JP2005/020470

C (続き) . 関連すると認められる文献		
引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 63-182758 A (日本電気株式会社) 1988. 07. 28, 全頁, 全図 (ファミリーなし)	1-12
A	JP 3-233792 A (日本電気オフィスシステム株式会社) 1991. 10. 17, 全頁, 全図 (ファミリーなし)	1-12